IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA
AT BECKLEY

ECHOSTAR SATELLITE L.L.C., a Colorado Corporation,
ECHOSTAR TECHNOLOGIES CORPORATION, a Texas Corporation, and

NAGRASTAR L.L.C., a Colorado Corporation, # 20045

Plaintiffs,

v. Civil Action No. 5:07-00096

WILLIAM A. ROLLINS, an Individual, a/k/a BILLY ROLLINS, a/k/a WILD SHARKY

Defendant.

ORIGINAL COMPLAINT

Plaintiffs EchoStar Satellite L.L.C., EchoStar Technologies Corporation, and NagraStar L.L.C. (collectively "EchoStar" or "Plaintiffs") file this Original Complaint against William Rollins a/k/a Bill Rollins, a/k/a Wild Sharky ("Rollins" or "Defendant") and, in support thereof, would respectfully show the Court the following:

NATURE OF THE ACTION

1. EchoStar is a multi-channel video provider, providing video, audio, and data services to customers throughout the United States, Puerto Rico, and

the U.S. Virgin Islands via a Direct Broadcast Satellite ("DBS") system. As part of that business, EchoStar uses high-powered satellites to broadcast, among other things, movies, sports, and general entertainment programming services ("EchoStar Programming") to consumers who have been authorized to receive such services after payment of a subscription fee (or in the case of a pay-per-view movie or event, the purchase price). EchoStar operates its DBS service under the trade name "DISH Network." The more than 12 million households and estimated 17 million viewers of DISH Network can obtain hundreds of channels of programming in digital video and CD-quality audio, all from an 18 to 20 inch satellite dish. EchoStar encrypts–electronically scrambles–its satellite transmission to prevent unauthorized viewing of its television programming. EchoStar, together with its affiliates, employs over 12,000 people in the United States.

2. EchoStar purchases the distribution rights for most of the EchoStar Programming it sells from program and content providers such as network affiliates, pay and specialty broadcasters, cable networks, motion picture distributors, sports leagues, event promoters, and other programming rights holders. EchoStar contracts and pays for the right to distribute EchoStar Programming to its subscribers, and holds rights to exhibit the EchoStar Programming to them.

3. EchoStar encrypts its satellite signals using technology provided by NagraStar. NagraStar is a joint venture between EchoStar and the Kudelski

Group, a group of companies headquartered in Switzerland. NagraStar, among other things, is a supplier of Access Cards with embedded microprocessors that are part of a larger "conditional access system" known as DNASP ("digital Nagra Advanced Security Process"). DNASP uses a complex encryption system that is combined with a Digital Video Broadcaster ("DVB") scrambler/encoder system to form EchoStar's management and security system (the "Security System"), which, among other things, protects EchoStar Programming from being viewed by unauthorized persons or entities. NagraStar provides DNASP to EchoStar under a license from the Kudelski Group.

4. The Security System, among other things, serves two interrelated functions: (1) subscriber management, allowing EchoStar to "turn on" programming that a customer has ordered; and (2) encryption, preventing individuals or entities who have not ordered programming from receiving it.

5. Defendant Rollins has violated federal laws by: (a) illegally circumventing the Security System; (b) aiding, assisting, and/or abetting others to illegally circumvent the Security System; (c) illegally publishing proprietary information about the Security System; and/or (d) designing, manufacturing, assembling, modifying, importing, exporting, possessing, distributing, publishing, posting and/or otherwise distributing devices and software designed or intended to facilitate the reception and decryption of EchoStar's encrypted satellite-delivered television programming service by persons not authorized to receive such programming.

6. The acts of Defendant, explained more fully below, violate the provisions of several federal statutes designed to prevent such unlawful conduct.

7. Plaintiffs seek damages and injunctive relief, as well as costs, including reasonable attorney fees.

PARTIES

8. Plaintiff EchoStar Satellite L.L.C., ("ES") is a Colorado corporation with its principal place of business at 5701 S. Santa Fe, Littleton, Colorado 80120.

9. Plaintiff EchoStar Technologies Corporation ("ETC") is a Texas corporation. Plaintiff ETC has its principal place of business at 90 Inverness Circle East, Englewood, Colorado 80112.

10. Plaintiff NagraStar L.L.C. ("NagraStar") is a joint venture and Colorado corporation with its principal place of business at 90 Inverness Circle East, Englewood, Colorado 80112.

11. Based upon information and belief, Defendant Rollins is a citizen and resident of Beckley, West Virginia whose principal residence is located at 231 Johnny Hollow Road, Beckley, West Virginia, 25007.

JURISDICTION AND VENUE

12. This case arises under the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-1205 and the Communications Act of 1934, as amended, 47 U.S.C. § 605.

13. This Court has subject matter jurisdiction over this case pursuant

to 28 U.S.C. §§ 1331 (federal question), 1332(a) (diversity), 1338 (copyright); 47 U.S.C. § 605(e)(3)(A); and 17 U.S.C. § 1203(b) (DMCA). Plaintiffs are Colorado Corporations, Defendant is a West Virginia resident, and the amount in controversy is in excess of $75,000.00, exclusive of costs and attorneys' fees.

14. This Court has personal jurisdiction over the Defendant in this action as Defendant is a citizen and resident of West Virginia.

FACTUAL ALLEGATIONS

15. Plaintiffs' allegations as to themselves and their own actions are based upon personal knowledge. Based upon reasonable and diligent investigative efforts, Plaintiffs believe that substantial evidentiary support exists for the allegations related to the Defendant herein or that such allegations are likely to have evidentiary support after a reasonable opportunity for further investigation and/or discovery.

EchoStar's Security System

16. EchoStar has invested several billion dollars to develop and deploy its distribution and broadcasting system. All programming distributed by EchoStar is delivered to one or both of its broadcast centers in Cheyenne, Wyoming, and Gilbert, Arizona, where it is digitized, compressed, and scrambled. EchoStar then transmits the scrambled signals to multiple satellites located in geo-synchronous orbit above the Earth.

17. EchoStar's satellites have relatively fixed "footprints" (i.e., a

terrestrial territory within which the scrambled satellite broadcast signals can be received). The "footprints" of the satellites used by EchoStar cover the United States, portions of Mexico, parts of Canada, and several Caribbean nations, and territories. The satellites relay the scrambled signals back to Earth, where they can be received by EchoStar's subscribers.

18. A consumer wishing to subscribe to EchoStar's DISH Network programming first must have the necessary equipment, which consists primarily of a satellite dish antenna and an integrated receiver/decoder, also called a "receiver" or a "set-top box." An EchoStar Access Card is necessary to operate the satellite receiver.

19. The credit card-sized "Access Card" is sometimes referred to as a "smart card." These Access Cards are sold by NagraStar to EchoStar.

20. The Access Card is inserted into a slot in the front of the set-top box and subscribers are not authorized to modify these cards. The Access Cards are provided by EchoStar for use in connection with the set-top box to the subscriber for the sole purpose of enabling authorized access to the DISH Network.

21. These Access Cards are essential to the operation of the DISH Network service because they contain a microprocessor chip that functions as a small computer, in the sense that the chip is a high speed data processing device that stores data and performs various computing functions. Most importantly, these microprocessors store certain encryption technology and communicate

with the set-top box to enable the decryption of the signal transmitted from EchoStar.

22. EchoStar frequently communicates with the microprocessor on the Access Card. The microprocessor receives and stores information from EchoStar; this information is routinely updated. The access card includes "customer information," such as the programming packages that the subscriber is entitled to view, as well as the encryption technology that allows an authorized subscriber to view these programs. The access card directs the set-top box to decrypt signals for the programs that the subscriber is authorized to view (e.g., basic packages, premium services, or pay-per-view movies or events).

23. Additionally, the microprocessor on the Access Card, in conjunction with the set-top box, is programmed to handle routine telecommunications over telephone lines with respect to viewer purchases of a pay-per-view movie or other event. These communications are essential to EchoStar's billing, accounting, and customer service. To enable these telecommunications initiated by the microprocessor to take place, EchoStar directs DISH Network subscribers to connect their set-top box to an open telephone line.

24. At the first activation of a customer's subscription, EchoStar sends a signal to the smart card in order to "pair" or "marry" the smart card to the receiver. Both smart card and receiver have a unique identification number that is maintained by EchoStar's subscriber management system. This pairing

operation utilizing the two unique identification numbers is mandatory for the proper operation of the Security System because certain secrets are contained in both the smart card and the set-top box.

25. One of the most important secrets contained in the set-top box are the DES keys (also called Box Keys), which are integral to the process of pairing a set-top box to an individual Access Card. These Box Keys are unique and individual to one, and only one, receiver. Once they are imprinted from the Receiver to the Smart card - done during the process of the first communication between EchoStar and the individual Receiver - they form the only "language" of communication that can be used for the Receiver to decrypt certain crucial information sent by EchoStar to the Receiver.

26. EchoStar added a JTAG port on the bottom of EchoStar's satellite receivers for use in the manufacturing process to load test software into the satellite receiver. The test software gets loaded into memory on the receiver and runs software diagnostic, among other things, on the satellite receiver's memory board and makes the receiver go through certain test paces while another computer on the outside of the receiver is checking patterns and telling the receiver to go to the next test. For example, the computer diagnostic that is run through the JTAG port tells the EchoStar satellite receiver to decode certain audio, test computer and satellite receiver functions, all the while doing this simultaneously. The JTAG port is also used by EchoStar in its service organization when EchoStar gets a satellite receiver back and needs to clean it

up and send it back out to the field. Importantly, there is absolutely no other legitimate use for this JTAG port. Specifically, the only use a non-EchoStar individual would have for these JTAG ports would be to 'pirate' a receiver.

27. The TSOP is part of the memory within the chip and it holds the "box key." The box key is used to identify whether a given card goes with a particular receiver. The box key functions as a pairing key and is used for communication from the smart card to the receiver. Essentially, each EchoStar receiver's unique Box key is a receiver-specific language that facilitates communication from a satellite signal to the receiver via the smart card. Because an EchoStar receiver's box key is fundamental in protecting the DISH Network programming from satellite piracy, these box keys are known only to authorized EchoStar personnel. Accordingly, when an authorized satellite receiver is added to the DISH Network system, based upon that receiver's identification, EchoStar knows what the secret box key is that is stored in that particular receiver's memory, and that is the key that will be used to de-scramble the messages from the smart card. EchoStar looks up the authorized user's identification number and can them determine the box key assigned to that receiver. Then, EchoStar's up-link center sends the secret number in an encrypted message to the authorized receiver's smart card so that the smart card will have the same key number in it. It is this process that allows the encrypted messages in the DISH Network signal to be sent from the smart card to the authorized receiver.

28. As detailed herein, EchoStar's Security System effectively controls access to copyrighted works included in DISH Network programming. In addition, the Security System ensures that the protection afforded to this copyrighted material, such as limitations on the dissemination and use in accordance with EchoStar's contractual agreements with content providers, is preserved.

The Black Market in Piracy Technology, Illegally-Modified DISH Access Cards and Programming Services, and EchoStar's Efforts to Combat Piracy

29. Various types of equipment and devices appear on the black market for the sole purpose of illegally descrambling or "pirating" EchoStar Programming. These devices initially consisted of printed circuit boards that when programmed, operated in the place of, and/or in conjunction with, DISH Access Cards. These devices compromised the DISH Security System by modifying and/or circumventing the security software in the DISH Access Cards. In addition to the various pirate devices, certain software, codes, commands, updates, patches, "fixes", and other technology support information is used to assist in the unlawful circumvention of EchoStar's security system and the resulting theft of EchoStar's programming.

30. EchoStar and NagraStar have developed anti-piracy divisions in an effort to combat the theft of EchoStar's programming. EchoStar's anti-piracy strategy includes the periodic introduction of new generations of DISH Access

Cards containing updated software that the pirates have not yet hacked. The first DISH Access Card was known as the ROM 2 card. EchoStar and NagraStar subsequently deployed DISH Access Cards with improved anti-piracy technologies, including the ROM 3, ROM 10, ROM 11, ROM 101, ROM 102, ROM S01, ROM S02 and ROM 206.

31. The main purpose of developing and introducing successive generations of DISH Access Cards is to foil hackers and render obsolete existing piracy devices. Converting EchoStar customers to new generations of DISH Access Cards and switching the satellite datastream so that it can only be received by the new DISH Access Cards requires the pirates to start over again in attacking the technology. EchoStar and NagraStar have invested and continue to invest significant time and money in these enhancements. EchoStar and NagraStar also update the DISH Access Cards to improve their functionality and service to EchoStar's customers.

32. EchoStar and NagraStar also invest heavily in developing and deploying countermeasures to maintain the integrity of the DISH Security System. Such countermeasures include electronic countermeasures ("ECM's"), which are periodically broadcast over the satellites to disable unauthorized DISH Access Cards.

33. Despite these improvements to the DISH Security System, piracy has continued to proliferate. Concurrently with the introduction of new

generations of DISH Access Cards, new sophisticated piracy devices and components thereof ("Pirate Boards") have appeared on the black market. These devices include so-called "AVR Boards" which are printed circuit boards containing a microprocessor, a parallel port connector, and a socket for a DISH Access Card, which permit a DISH Access Card to be inserted into the socket and the AVR board itself inserted into the receiver. The AVR board microprocessor can be programmed with piracy software to enable the receiver to descramble EchoStar Programming. Newer versions of Pirate Boards can even be programmed and used without a DISH Access Card.

34. Other devices available on the black market include "programmers" and "loaders" whose only known purpose is to enable hackers to re-program and modify DISH Access Cards and Pirate Boards to circumvent the DISH Security System. These types of devices are particularly damaging to EchoStar because an individual with such a device can: (1) repeatedly modify a DISH Access Card, (2) modify numerous DISH Access Cards, and re-sell them to other persons, and (3) program and/or modify Pirate Boards to steal EchoStar Programming.

35. Piracy software is an essential component of most piracy devices. Among the software offered on piracy web sites today is software that is created and offered solely for the purpose of "programming", "cracking", "flashing" and "modifying" DISH Access Cards, receivers, or Pirate Boards, or "repairing", "patching", or "fixing" illegally-modified DISH Access Cards, receivers, or Pirate

Boards that have been disabled by ECM's. This software is known by such names as "NagraEdit", "rf040", "BAPA_BELL", "Space Twister" and "ROM Tier Maker." Piracy web sites often restrict access to piracy software to persons who pay fees to become "members" or "subscribers".

36. Pirates often refer to the use of modified DISH Access Cards, Pirate Boards, or hardware as "testing" (implying that they are used for the purpose of "testing" the Receiving Equipment). EchoStar does not authorize anyone to modify, alter, reprogram or "test" its Receiving Equipment for any purpose whatsoever. Legitimate subscribers to EchoStar would have no reason to "test", tamper with, or alter the Receiving Equipment. Rather, the sole purpose of such activities would be to circumvent the DISH Security System to steal EchoStar Programming.

37. Some piracy devices are sold pre-programmed with piracy software. However, in an effort to avoid prosecution, many satellite pirates offer only "unprogrammed" or "unflashed" piracy devices for sale to consumers. In such cases the pirates will suggest that the piracy devices they offer for sale are "legitimate" or "legal" because the purchaser must obtain piracy software from other sources and program them before they can be used for piracy. Pirates will generally refer their customers to sources of software components either verbally, by e-mail or by way of links to software providers' web sites.

38. Many pirates also offer services in support of the piracy devices and

the piracy software that they sell. These services include:

(a) access card programming services by which DISH Access Cards are re-programmed by pirates to permit them to be used for piracy purposes;

(b) box key "extraction" services by which Box Keys are obtained from receivers, to be used in "pairing" the receivers to DISH Access Cards supplied by pirates; and

(c) "unlocking" services by which receivers and DISH Access Cards that have been "paired" together can be "unlocked", thereby permitting the receiver or DISH Access Card to be used with a DISH Access Card or receiver other than the one to which it has been "paired"

39. The ongoing provision of new versions of piracy software and the aforementioned services results in continual losses for EchoStar.

40. The black market in Piracy Technology represents a multimillion-dollar industry in Canada and the United States. The pirates who fuel this black market are geographically dispersed and typically operate individually or within a very small group. Pirates can start up businesses with a minimal investment of capital and other resources, and typically operate as "fly-by-night" businesses with few assets and are able to shut down or relocate with ease. By using the Internet, pirates are able to operate without regard to national borders and reach millions of potential customers. The identities of pirates who develop, manufacture, and distribute Piracy Technology are known

only to a few. Locating their places of business and web sites is often a difficult and time-consuming undertaking.

41. Pirates are generally aware of the illegal nature of their activities, and often take steps to avoid detection and to conceal the evidence of their wrongdoing. For example, pirates who operate retail storefront premises often keep little inventory in the premises, with the balance being stored at storage facilities, in neighbouring businesses, or at their residences or those of their relatives or associates. Pirates who operate Internet-based businesses benefit from the anonymity which the Internet provides, and often locate the servers containing their web sites' databases in undisclosed (and sometimes offshore) locations, and use third party on line payment processors that store their sales records elsewhere. Pirates can access their web sites by "remote access" from their residences, and in many cases orders received by their web sites are automatically e-mailed to the pirates or their associates who can invoice, package and ship the orders from wherever the Piracy Technology is being stored.

The Sale and Use of Free-To-Air Receivers for Satellite Piracy

42. In 2003, pirates developed a new way to steal EchoStar Programming by using so called "free-to-air" receivers ("FTA receivers") that had been programmed with piracy software. FTA receivers are designed to receive "free-to-air" satellite television signals, which are either not scrambled or scrambled but available free of charge. There are numerous "free-to-air"

television channels available in Canada and the United States, including many ethnic, religious, business, music, information and advertisement channels. "Free-to-air" channels and FTA receivers have existed for many years, and are today manufactured and sold by several companies under various brand names including "Ariza", "BlackBird", "Fortec", "Pansat", "Coolsat", "Dreambox", "Coship", and "Topfield".

43. FTA receivers are similar to the receivers used by EchoStar in that they are a set-top box, approximately the size of a VCR player, which contains descrambling circuits and software which enables them to perform their function. Some FTA receivers also contain an access card reader.

44. EchoStar and NagraStar believe that pirates acquire, modify, and sell FTA receivers for piracy purposes as follows:

(a) pirates obtain the FTA receivers from their manufacturers or elsewhere, and then load piracy software onto the circuit chips contained within them;

(b) once an FTA receiver has been modified with piracy software, it can receive and descramble EchoStar Programming without authorization from or payment to EchoStar; and

(c) pirates then sell the modified FTA receivers to their customers.

45. In some cases, pirates do not load piracy software onto the FTA receivers themselves but rather direct their customers to any of the numerous web sites that offer piracy software for download. The modification of FTA

receivers for piracy purposes represents a serious threat to EchoStar and NagraStar. The purchaser of an FTA receiver can run any software that he or she wishes on the FTA receiver. Because FTA receivers are not manufactured or sold by EchoStar and NagraStar to receive EchoStar Programming, these companies have no control over the software contained in them. As a result, security measures such as ECM's transmitted by EchoStar and NagraStar through their satellite datastream may have no effect on these modified FTA receivers. EchoStar and NagraStar may therefore be unable to attack or disable modified FTA receivers in the same way that they can with legitimate receivers that are being used and modified for piracy purposes.

46. The modification and sale of FTA receivers for piracy purposes represents a new stage in the evolution of Piracy Technology against EchoStar and NagraStar. Because FTA receivers and the use of them are legal, in certain circumstances, in Canada and the United States, they are attractive to pirates as a "legal" product with which to engage in piracy activities. This cloak of legitimacy presents serious challenges to EchoStar and NagraStar in their enforcement activities.

The DISH Network Logo

47. In 1996, EchoStar created its distinctive logo, which consists in part of a stylized satellite emanating a television broadcast signal while in orbit around the Earth, which also forms a stylized letter "I" (the "DISH Network Logo").

The DISH Network Logo features prominently in all marketing and promotional materials prepared by EchoStar, in all communications emanating from EchoStar, and on most satellite dishes used to receive EchoStar Programming which are sold to consumers. EchoStar registered trademarks for the DISH Network Logo in the United States and Canada. EchoStar is the holder of Canadian registered trademarks TMA 636 661 and TMA 636 437 for the DISH Network Logo.

"Forum" and Chat Web Sites

48. Many pirates also operate or participate in piracy web sites that serve as a "forum" for the dissemination and exchange of information pertaining to Piracy Technology and satellite piracy generally. In some cases, forum sites do not sell any Piracy Technology themselves. Rather, they provide information and instruction on the use of Piracy Technology and provide links to other piracy web sites that sell Piracy Technology and related services to permit consumers to unlawfully obtain EchoStar's programming.

49. It is typical for forum sites to receive advertising revenue from other piracy web sites that place advertisements or links on them. Alternatively, some pirates operate forum sites to establish credibility in the piracy community and obtain a loyal group of users who they then refer to other web sites operated by that pirate to purchase Piracy Technology.

50. Among the software offered on these "forum" sites today is software

that is created and offered solely for the purpose of "programming", "cracking", "flashing", "fixing", or "updating" illegally modified DISH Access Cards, receivers or Pirate Boards that have been disabled by an ECM.

Defendant's Wrongful Conduct

51. Upon information and belief, Defendant Rollins is engaged in the facilitation of satellite television piracy with respect to EchoStar's DISH Network programming and NagraStar's conditional access system ("CAS").[1]

52. Defendant Rollins is and has been engaged in marketing, selling, and distributing Piracy Technology and services in support thereof, designed to steal EchoStar Programming. In particular, in the course of carrying on their business and undertaking, Defendant Rollins has:

(a) sold, distributed, provided, trafficked in, exposed and offered Piracy Technology and components thereof, including Cyclone Unlockers, Atmega 128s, Jtags, ISO Programmers, modified Access Cards, FTA receivers, and piracy software;

(b) sold, distributed, provided, trafficked in, exposed and offered services in support of Piracy Technology;

(c) operated the Web Sites to advertise, promote, sell and facilitate the sale of Piracy Technology and services in support thereof;

1 Plaintiffs are further informed and believe that Defendant Rollins has been, and is currently actively involved in the facilitation of others in the unlawful circumvention and signal theft of encrypted programming provided by Bell Express View ("BEV") in Canada. BEV also uses encryption technologies and services provided in part by NagraStar and one of its joint-owners (the Kudelski Group SA, based in Switzerland). Nothing contained herein is meant to, nor does constitute any waiver of rights held by either BEV or Kudelski with respect to Defendant's unlawful conduct.

(d) offered advice, assistance, and instructional information on Piracy Technology through the Web Sites and otherwise to permit customers to steal EchoStar Programming; and/or

(e) assisted, encouraged, aided, and/or abetted other persons in carrying out these and other similar activities.

53. Defendant has or is actively engaged in the publication, distribution or otherwise trafficking in codes, commands, software, programs and/or other devices that permit the illegal and unauthorized reception and decryption of DISH Network programming. Defendant has acted and continues to act with intent to design, produce, publish, and distribute equipment and software, along with instructions and directions as to its installation, activation, and maintenance with the primary purpose of circumventing EchoStar's Security System and obtaining the unauthorized interception of DISH Network satellite signals without paying for it.

54. Defendant's unlawful conduct of developing, distributing, providing technical support for, and otherwise trafficking in various codes, commands, software, programs and other signal theft devices which facilitates, aides and abets others in the theft of DISH Network programming to which they do not subscribe and for which they do not pay. Defendant has sold, provided, or trafficked in these devices for valuable consideration thereby allowing purchasers to obtain unauthorized access to DISH Network programming. Defendant has marketed, advertised, and conducted business via the Internet in

the State of Colorado. Additionally, Defendant has engaged in communications (either directly or via publications on various pirate-related internet sites) with Colorado residents in his unauthorized efforts to market, sell, and distribute the pirated (unlawfully modified and/or accessed) EchoStar satellite Receivers, EchoStar/NagraStar modified original smart cards ("MOSC"), codes, commands, software, programs and other signal theft devices forming the basis of EchoStar's claims. Defendant's direct contacts with Colorado residents constitutes a purposeful availment to the benefits and protections of the State of Colorado. Moreover, EchoStar's action arises from and is directly related to Defendant's unlawful contacts with the State of Colorado.

55. Defendant Rollins has used various internet aliases, email addresses, screen names or other pseudonyms such as: (a) Wild Sharky; (b) wildsharky80@hotmail.com; (c) info@proone-fta.net; and/or (d) WildSharky3680 to publish, post, distribute, transfer, provide technical support for, or otherwise traffic in various codes, commands, software or programs designed to facilitate, aide and/or abet others in the unauthorized reception and decryption of EchoStar's encrypted copyrighted programming. Defendant has used these aliases, email addresses, screen names or other pseudonyms to publish, post, transfer, provide technical support for, or otherwise traffic in these codes, commands, software or programs via pirate-related internet websites such as www.tomico-satellites.com;

www.pro-kings.net; and www.proone-fta.net, among others.

56. Defendant Rollins facilitation of the wide-spread theft of EchoStar's programming has resulted, and continues to result in significant injuries to Plaintiffs for which they now seek redress.

Defendant's facilitation of the theft of EchoStar's programming causes irreparable harm

57. The conduct of Defendant Rollins has caused significant and irreparable harm to the Plaintiffs. In particular, Defendant Rollins' actions in facilitating the theft of EchoStar's programming has:

(a) deprived EchoStar of an incalculable number of existing and prospective customers, as a result of the inability to ascertain, trace or account for all uses of EchoStar's programming;

(b) caused EchoStar a loss of revenues, proceeds, profits and other benefits that is also incalculable, because it is difficult for EchoStar to trace, calculate or prove:

(i) how many persons are receiving its programming without authorization;

(ii) how much and which type of programming and how much pay-per-view programming these persons are receiving without authorization;

(iii) the actual value of the programming being received without authorization;

(c) caused EchoStar to lose the amounts which it pays to subsidize the cost of receivers (in the expectation that its subsidy will promote legitimate subscriptions), for every receiver which "disappears" into the black market;

(d) exploited for commercial gain the Plaintiffs' trade secrets and confidential information in their security system;

(e) jeopardized the goodwill associated with EchoStar's name and reputation in the marketplace, which in turn results in continuous losses of revenue, proceeds, profits and other benefits that are impossible to ascertain at this time; and

(f) damaging the business relationships and good reputation that the Plaintiffs have developed over many years

CAUSES OF ACTION

FIRST CAUSE OF ACTION
(Circumventing Technological Measures Concerning Protected and Copyrighted Works in Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(1)(A))

58. Plaintiffs re-allege and incorporate the above paragraphs as if fully set forth in this cause of action.

59. Defendant circumvented and/or assisted other persons to circumvent Plaintiffs' technological measures contained within EchoStar Access Cards and/or Receivers which effectively control access to works protected under Title 17 of the United States Code, namely DISH Network's satellite television programming services and the protected works broadcasted thereon, by altering,

modifying, compromising, pirating, reprogramming, blocking and/or otherwise interfering with the intended operation of EchoStar Access Cards and/or Receivers to bypass EchoStar's encryption protection contained therein and to enable the unauthorized access of copyrighted satellite television programming, with each instance in violation of 17 U.S.C. § 1201(a)(1)(A).

60. Defendant's acts of circumvention and assisting others to circumvent have been and continue to be performed without the permission, authorization, or consent of Plaintiffs or any owner of copyrighted programming broadcasted on the DISH Network.

61. Defendant has violated Section 1201(a)(1) of the Digital Millennium Copyright Act willfully, and for purposes of commercial advantage or private financial gain.

62. Pursuant to 17 U.S.C. § 1203, Plaintiffs are entitled to equitable relief, damages (either statutory damages of $200 to $2,500 per violation, or actual damages plus any profits realized by Defendant as a result of this unlawful conduct), reasonable attorney's fees, and costs, in addition to all other relief to which they may be entitled.

63. Defendant's violations have caused and will continue to cause Plaintiffs irreparable harm, and Plaintiffs have no adequate remedy at law to redress any such continued violations. Unless restrained by this Court, Defendant will continue to violate 17 U.S.C. § 1201(a)(1).

SECOND CAUSE OF ACTION
(Trafficking and Manufacturing Signal Theft Devices to Circumvent Technological Measures Restricting Access to the DISH Network in Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2))

64. Plaintiffs re-allege and incorporate the above paragraphs as if fully set forth in this cause of action.

65. Defendant was and is actively engaged in the business of developing, manufacturing, importing, offering to the public, providing, or otherwise trafficking in altered, modified, compromised, and/or counterfeit EchoStar Access Cards and/or Receivers and other circumvention or signal theft devices, including various codes, commands, software and programs designed to enable users to illegally modify or alter EchoStar Access Cards, Receivers, and/or Plaintiffs' Security System knowing, or having reason to know, that such signal theft devices: (a) are primarily designed or produced for the purpose of circumventing Plaintiffs' encryption and conditional access technological measures that effectively control access to copyrighted satellite television programming; (b)have only limited commercially significant purpose or use other than to circumvent Plaintiffs' encryption and conditional access technological measures that effectively controls access to copyrighted programming; or (c) were marketed by Defendant, or others acting in concert with Defendant with Defendant's knowledge, for use in circumventing Plaintiffs' encryption and conditional access technological measures Plaintiffs' encryption and conditional access technological measures that effectively controls access to copyrighted

programming, in violation of 17 U.S.C. § 1201(a)(2).

66. Defendant's violations have injured, and will continue to injure, Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and other valuable consideration, compromising Plaintiffs' security and accounting systems, infringing Plaintiffs' trade secrets and proprietary information, and interfering with Plaintiffs' contractual and prospective business relations.

67. Defendant's acts of circumvention, including the facilitation of circumvention, have been, and continue to be, performed without the permission, authorization, or consent of Plaintiffs or any owner of copyrighted programming.

68. Defendant has violated Section 1201(a)(2) of the Digital Millennium Copyright Act willfully, and for purposes of commercial advantage or private financial gain.

69. Pursuant to 17 U.S.C. § 1203, Plaintiffs are entitled to equitable relief, damages (either statutory damages of $200 to $2,500 per violation, or actual damages plus any profits realized by Defendant as a result of this unlawful conduct), reasonable attorney's fees, and costs, in addition to all other relief to which they may be entitled.

70. Plaintiffs have been damaged by Defendant's actions in an amount to be proven at trial.

71. Such violations have caused, and will continue to cause, Plaintiffs irreparable harm, and Plaintiffs have no adequate remedy at law to redress any

such continued violations. Unless restrained by this Court, Defendant will continue to violate 17 U.S.C. § 1201(a)(2).

THIRD CAUSE OF ACTION
(Manufacture of and Traffic in Signal Theft Devices in Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(b)(1))

72. Plaintiffs re-allege and incorporate the above as if fully set forth in this cause of action.

73. Defendant was and is actively engaged in the business of developing, manufacturing, importing, offering to the public, providing, or otherwise trafficking in altered, modified, compromised, and/or counterfeit EchoStar Access Cards and/or Receivers and other circumvention or signal theft devices, including various codes, commands, software and programs designed to enable users to illegally modify or alter EchoStar Access Cards, Receivers, and/or Plaintiffs' Security System knowing, or having reason to know, that such signal theft devices: (a) are primarily designed or produced for the purpose of circumventing the protection afforded by Plaintiffs' encryption and conditional access technological measures that effectively protects rights of copyright owners in a work or portion thereof; (b) have only limited commercially significant purpose or use other than to circumvent the protection afforded by Plaintiffs' encryption and conditional access technological measures that effectively protects rights of copyright owners in a work or portion thereof; or (c) were marketed by Defendant, or others acting in concert with Defendant with

Defendant's knowledge, for use in circumventing Plaintiffs' encryption and conditional access technological measures Plaintiffs' encryption and conditional access technological measures that effectively protects rights of copyright owners in a work or portion thereof, in violation of 17 U.S.C. § 1201(b)(1).

74. Defendant's violations have injured, and will continue to injure, Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and other valuable consideration, compromising Plaintiffs' security and accounting systems, infringing Plaintiffs' trade secrets and proprietary information, and interfering with Plaintiffs' contractual and prospective business relations.

75. Defendant's acts of circumvention have been, and continue to be, performed without the permission, authorization, or consent of Plaintiffs or any owner of copyrighted programming.

76. Defendant has violated Section 1201(b)(1) of the Digital Millennium Copyright Act willfully, and for purposes of commercial advantage or private financial gain.

77. Pursuant to 17 U.S.C. § 1203, Plaintiffs are entitled to equitable relief, damages (either statutory damages of $200 to $2,500 per violation, or actual damages plus any profits realized by Defendant as a result of this unlawful conduct), reasonable attorney's fees, and costs, in addition to all other relief to which they may be entitled.

78. Such violations have caused, and will continue to cause, Plaintiffs irreparable harm, and Plaintiffs have no adequate remedy at law to redress any such continued violations. Unless restrained by this Court, Defendant will continue to violate 17 U.S.C. § 1201(b)(1).

FOURTH CAUSE OF ACTION
(Facilitating the Unauthorized Reception of Satellite Signals in Violation of the Communications Act of 1934, as amended, 47 U.S.C. § 605(a))

79. Plaintiffs re-allege and incorporate the above as if fully set forth in this cause of action.

80. By designing, manufacturing, developing, manufacturing, assembling, modifying, trafficking, distributing, and/or selling EchoStar Access Cards, Receivers, and/or other circumvention or signal theft devices, including various codes, commands, software and programs designed to enable users to illegally modify or alter EchoStar Access Cards, Receivers, and/or Plaintiffs' Security System Defendant has assisted the unauthorized reception of use of EchoStar's satellite transmissions of television programming by persons not authorized to receive such transmissions, in violation of 47 U.S.C. § 605(a).

81. Defendant's violations have injured, and will continue to injure, Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and other valuable consideration, compromising Plaintiffs' security and accounting systems, infringing Plaintiffs' trade secrets and proprietary information, and interfering with Plaintiffs' contractual and prospective business relations.

82. Defendant's violations of 47 U.S.C. § 605(a) have injured, and will continue to injure, EchoStar's ability to maximize the revenues which it seeks to derive from its satellite television programming as EchoStar has been deprived of the benefit of subscribers to EchoStar's satellite television programming.

83. Defendant's acts of circumvention and the facilitation of circumvention have been, and continue to be, performed without the permission, authorization, or consent of Plaintiffs or any owner of copyrighted programming

84. Defendant has violated Section 605(a) the Communications Act willfully, and for purposes of commercial advantage or private financial gain.

85. Defendant knew, or should have known, that assisting third person in the reception and use of EchoStar's satellite transmissions of television programming, without authorization, was and is illegal and prohibited.

86. Pursuant to 47 U.S.C. § 605(e)(3), Plaintiffs are entitled to equitable relief, damages (either statutory damages of $1,000 to $10,000 per violation, or actual damages plus any profits realized by Defendant for each violation of 47 U.S.C. § 605(a)), and reasonable attorney's fees and costs. Plaintiffs seek all other relief to which they may be entitled.

87. Such violations have caused, and will continue to cause, Plaintiffs irreparable harm, and Plaintiffs have no adequate remedy at law to redress any such continued violations. Unless restrained by this Court, Defendant will continue to violate 47 U.S.C. § 605(a).

FIFTH CAUSE OF ACTION
(Manufacture and Sale of Signal Theft Devices in Violation of the Communications Act of 1934, as amended, 47 U.S.C. § 605(e)(4))

88. Plaintiffs re-allege and incorporate the above as if fully set forth in this cause of action.

89. Defendant has engaged in the business of manufacturing, assembling, modifying, importing (to the United States), exporting, selling, and distributing EchoStar Access Cards, Receivers, and/or other circumvention or signal theft devices designed to enable users to illegally modify or alter EchoStar Access Cards, Receivers, and/or Plaintiffs' Security System knowing, or having reason to know, that such signal theft devices are primarily of assistance in the unauthorized decryption of EchoStar's satellite television programming services, or are intended by Defendant to assist other persons in the unauthorized reception and use of EchoStar's satellite television programming services, in violation of 47 U.S.C. § 605(e)(4).

90. Defendant's acts of circumvention have been, and continue to be, performed without the permission, authorization, or consent of Plaintiffs or any owner of copyrighted programming.

91. Defendant's violations have injured, and will continue to injure, Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and other valuable consideration, compromising Plaintiffs' security and accounting

systems, infringing Plaintiffs' trade secrets and proprietary information, and interfering with Plaintiffs' contractual and prospective business relations.

92. Defendant has violated Section 605(e)(4) the Communications Act willfully and for purposes of commercial advantage or private financial gain.

93. Pursuant to 47 U.S.C. § 605(e)(3), Plaintiffs are entitled to equitable relief, damages (either statutory damages of $1,000 to $10,000 per violation, or actual damages plus any profits realized by Defendant for each violation of 47 U.S.C. § 605(a)), and reasonable attorney's fees and costs. Plaintiffs seek all other relief to which they may be entitled.

94. Such violations have caused, and will continue to cause, Plaintiffs irreparable harm, and Plaintiffs have no adequate remedy at law to redress any such continued violations. Unless restrained by this Court, Defendant will continue to violate 47 U.S.C. § 605(e)(4).

SIXTH CAUSE OF ACTION
(Unauthorized Interception of Electronic Communications in Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1)(a))

95. Plaintiffs re-allege and incorporate the above as if fully set forth in this cause of action.

96. By designing, developing, manufacturing, assembling, modifying, exporting, trafficking, selling, and distributing EchoStar Access Cards, Receivers, and/or other circumvention or signal theft devices, including various codes, commands, software and programs designed to enable users to illegally modify

or alter EchoStar Access Cards, Receivers, and/or Plaintiffs' Security System and advertising and providing software, information, and technical support services relating to EchoStar Access Cards, Receivers, and/or other circumvention or signal theft devices designed to enable users to illegally modify or alter EchoStar Access Cards, Receivers, and/or Plaintiffs' Security System Defendant intentionally intercepted, endeavored to intercept, or procured other persons to intercept or endeavor to intercept, EchoStar's satellite transmissions of television programming, in violation of 18 U.S.C. § 2511(1)(a).

97. Defendant's violations have injured, and will continue to injure, Plaintiffs by depriving Plaintiffs of subscription and pay-per-view revenues and other valuable consideration, compromising Plaintiffs' security and accounting systems, infringing Plaintiffs' trade secrets and proprietary information, and interfering with Plaintiffs' contractual and prospective business relations.

98. Defendant has engaged in conduct in violation of Section 2511(1)(a) of the Electronic Communications Privacy Act for a tortious or illegal purpose, or for purposes of direct or indirect commercial advantage or private commercial gain.

99. Defendant knew, or should have known, that such interception of EchoStar's satellite transmissions of television programming was and is illegal and prohibited.

100. Such violations have caused and will continue to cause Plaintiffs irreparable harm and Plaintiffs have no adequate remedy at law to redress any such continued violations. Unless restrained by this Court, Defendant will continue to violate 18 U.S.C. § 2511(1)(a).

SEVENTH CAUSE OF ACTION
(Trademark Infringement
in Violation of the Lanham Act, 15 U.S.C. § 1114)

101. Plaintiffs re-allege and incorporate the above as if fully set forth in this cause of action.

102. EchoStar has adopted the mark "DISH Network" and used it in interstate commerce for equipment, goods, and services sold or licensed by EchoStar as part of its direct broadcast satellite system. On February 5, 1995, an application for registration of said mark was filed in the United States Patent and Trademark Office. On May 5, 1998, said mark was registered in the United States Patent and Trademark Office on the Principal Register under the Act of 1946 covering the use of said mark on equipment, goods, and services sold or licensed by EchoStar as part of its direct broadcast system. EchoStar's registration is now outstanding and valid.

103. Defendant has infringed EchoStar's mark in interstate and foreign commerce by various acts including, but not limited to, designing, manufacturing, importing, distributing, selling, offering for sale, and advertising EchoStar Access Cards, Receivers, and/or other circumvention or signal theft

devices designed to enable users to illegally modify or alter EchoStar Access Cards, Receivers, and/or Plaintiffs' Security System under the name and mark of "DISH Network." Defendant's use of EchoStar's mark is without permission or authority of EchoStar and said use is likely to cause confusion, mistake, and deceit.

104. Defendant knew, or should have known, that their use of the "DISH Network" mark (1) on EchoStar Access Cards, Receivers, and/or other circumvention or signal theft devices that Defendant designed, manufactured, imported (to the United States), distributed, and sold, (2) on other circumvention or signal theft devices designed to enable users to illegally modify or alter EchoStar Access Cards, Receivers, and/or EchoStar's Security System that Defendant designed, manufactured, imported (to the United States), distributed, and sold, and (3) on Defendant's advertisements for the sale and use of EchoStar Access Cards, Receivers, and/or other circumvention or signal theft devices was and is illegal and prohibited.

105. Such violations have caused and will continue to cause Plaintiffs irreparable harm, and Plaintiffs have no adequate remedy at law to redress any such continued violations. Unless restrained by this Court, Defendant will continue to violate 15 U.S.C. § 1114.

EIGHTH CAUSE OF ACTION
(Use of False Designation
in Violation of the Lanham Act, 15 U.S.C. § 1125(a))

106. Plaintiffs re-allege and incorporate the above as if fully set forth in this cause of action.

107. Defendant has caused altered and/or modified EchoStar Access Cards, Receivers, and/or other circumvention or signal theft devices to enter into interstate and foreign commerce with the designation and representation "DISH Network" connected therewith. Defendant's use of "DISH Network" is a false designation of origin which is likely to cause confusion, mistake, and deceit as to the affiliation, connection, or association of Defendant with EchoStar and as to the origin, sponsorship, or approval of such goods and services by EchoStar.

108. Defendant's actions are in violation of 15 U.S.C. § 1125(a) in that Defendant has used in connection with goods and services advertised and sold by Defendant a false designation of origin, a false or misleading description and representation of fact which is likely to cause confusion, mistake, and deceit as to the affiliation, connection, or association of Defendant with EchoStar and as to the origin, sponsorship, or approval of Defendant's goods, services, and commercial activities by EchoStar.

109. Defendant knew, or should have known, that the false designation of origin and the false or misleading description and representation of fact was and is illegal and prohibited.

110. Such violations have caused and will continue to cause Plaintiffs irreparable harm, and Plaintiffs have no adequate remedy at law to redress any

such continued violations. Unless restrained by this Court, Defendant will continue to violate 15 U.S.C. § 1125(a).

PRAYER FOR RELIEF

WHEREFORE, premises considered, Plaintiffs demand a trial by jury and seek a judgment against Defendant as follows:

A. For a grant of preliminary and permanent injunctive relief restraining and enjoining Defendant and his employees, agents, representatives, attorneys, and all other persons acting or claiming to act on their behalf or under Defendant's direction or authority, and all persons acting in concert or in participation with Defendant, from:

(1) manufacturing, importing, offering to the public, providing, modifying or otherwise trafficking in any EchoStar Receiver that has been modified without authorization (including any Access Cards that have been modified without authorization), any satellite pirating device regardless of form, or any other technology, product, service, device, component, or part thereof, that:

(a) is primarily designed or produced for the purpose of circumventing the encryption access control protection contained in the software on Plaintiffs' Access Cards, contained within Plaintiffs' set-top boxes, or any other technological measure adopted by Plaintiffs that effectively controls access

to copyrighted programming or effectively protects the exclusive rights afforded the owners of copyrighted programming;

(b) has only limited commercially significant purpose or use other than to circumvent Plaintiffs' encryption access control protection, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted programming or effectively protects the exclusive rights afforded the owners of copyrighted programming;

(c) is knowingly marketed by Defendant and/or others acting in concert with him for use in circumventing Plaintiffs' encryption access control protection, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted programming oar effectively protects the exclusive rights afforded the owners of copyrighted programming; and

(2) assembling, modifying, selling, advertising, marketing, possessing, transporting and/or distributing through any means whether via the Internet or otherwise, any EchoStar receiver or Access Card that has been modified without authorization or any other electronic, mechanical, or other devices, the design of which renders them primarily useful for the purpose of the surreptitious interception of electronic communications.

B. For an Order impounding all of Plaintiffs' Access Cards, Receivers, and/or signal theft devices that have been modified without authorization, reprogramming equipment, and equipment used in the alteration and/or

modification of said devices that are in the possession, custody, or control of Defendant or his employees, agents, representatives, attorneys, and all other persons acting or claiming to act on their behalf or under Defendant's direction or authority, and all persons acting in concert or in participation with Defendant, that the Court has reasonable cause to believe were involved in a violation of either 17 U.S.C. § 1201, 47 U.S.C. § 605, 18 U.S.C. § 2511, 15 U.S.C. § 1114, or 15 U.S.C. § 1125(a).

C. For an Order requiring Defendant to post a prominent public notice on any and all Internet web sites owned, originated, operated, or controlled by Defendant, notifying all persons in possession of altered or modified Access Cards, Receivers, or other circumvention or signal theft devices that said items have been recalled and that they should be sent to EchoStar or destroyed;

D. For an Order requiring Defendant to identify all John Does working in concert with Defendant in performing the unlawful acts described herein, and to use all contact information in their possession to notify anyone that has obtained an altered or modified Access Card, Receiver, and/or other circumvention or signal theft device from Defendant that said items have been recalled and that they should be sent to EchoStar or destroyed;

E. For an Order directing Defendant to preserve and maintain all records, in any form (including electronic form), that evidence, refer or related to: altered or modified Access Cards, Receivers, or other unlawful devices, as

described herein; communications or correspondence with suppliers or customers of pirating devices, software, hardware or other equipment or know-how concerning access card programming, box key extraction; the identity of any manufactures, suppliers or customers of access card programming, box key extraction or set-top box modification programming services; and the quantity of all such devices in inventory and sold by Defendant;

F. For an Order permitting Plaintiffs, through their counsel, to inspect and make mirror image copies of any computer or electronic storage drives or back up tapes in the possession, custody, or control of Defendant or his employees, agents, representatives, attorneys, and all other persons acting or claiming to act on their behalf or under Defendant's direction or authority, and all persons acting in concert or in participation with Defendant that contain information related to Defendant's sales of unlawfully altered or modified EchoStar Access Cards, Receivers, or other unlawful devices, as described herein;

G. For an Order requiring Defendant to file with the Court and to serve on counsel for Plaintiffs within thirty (30) days from the entry of the injunction a report in writing under oath setting forth in detail the manner and form in which Defendant has complied with the Injunctions and Orders, as described in paragraphs A through F above;

H. Award Plaintiffs the greater of their actual damages together with any profits made by Defendant that are attributable to the violations alleged herein, or statutory damages in the amount of up to $100,000 for each violation of 47 U.S.C. § 605 (e) (4), pursuant to 47 U.S.C. § 605 (e) (3) (C) (I);

I. Award Plaintiffs the greater of their actual damages together with any profits made by Defendant that are attributable to the violations alleged herein, or statutory damages in the amount of up to $2,500 for each violation of 17 U.S.C. § 1201(a) (1), (a)(2), and (b)(1), pursuant to 17 U.S.C. § 1203(c)(2) and (3)(A);

J. Award Plaintiffs the greater of their actual damages together with any profits made

by Defendant as a result of the violations alleged herein, or statutory damages of whichever is the greater of $100 a day for each day of violation of 18 U.S.C. §§ 2511(1)(a), or $10,000, pursuant to 18 U.S.C. § 2520(c)(2);

K. Award Plaintiffs punitive damages for each violation of 18 U.S.C. §§ 2511(1)(a),

pursuant to 18 U.S.C. § 2520(b)(2);

L. For an Order freezing all of Defendant's assets pending an accounting and restitution by Defendant of all gains, profits, and advantages derived from Defendant's unlawful activities;

M. For an award of Plaintiffs' costs, reasonable attorneys' fees, and investigative fees.

N. Prejudgment interest on all profits and damages granted by this Court; and

O. Any such further and other relief Plaintiffs are justly entitled as determined by the Court.

JURY TRIAL DEMANDED

ECHOSTAR SATELLITE L.L.C.,
ECHOSTAR TECHNOLOGIES CORPORATION, and
NAGRASTAR L.L.C.,

By counsel,

Christopher J. Sears (WV Bar #8095)
Shuman, McCuskey & Slicer, PLLC
1411 Virginia Street East, Suite 200
Post Office Box 3953
Charleston, WV 25339
(304) 345-1400

and

Chad M. Hagan (*pro hac vice* to be filed)
T. WADE WELCH & ASSOCIATES
2401 Fountainview, Suite 700
Houston, Texas 77057
(713) 952-4334